



CVE-2014-3149

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2014-3149
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-07-03 14:55:00 UTC
Updated	2020-06-03 14:54:00 UTC
Description	Cross-site scripting (XSS) vulnerability in Invision Power IP.Board (aka IPB or Power Board) 3.3.x and 3.4.x through 3.4.6, ,

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Invisioncommunity	Invision Power Board	3.3.0	All	All	All
Application	Invisioncommunity	Invision Power Board	3.3.0	alpha1	All	All
Application	Invisioncommunity	Invision Power Board	3.3.0	alpha2	All	All
Application	Invisioncommunity	Invision Power Board	3.3.0	beta1	All	All
Application	Invisioncommunity	Invision Power Board	3.3.0	beta2	All	All
Application	Invisioncommunity	Invision Power Board	3.3.0	beta3	All	All
Application	Invisioncommunity	Invision Power Board	3.3.0	beta4	All	All
Application	Invisioncommunity	Invision Power Board	3.3.1	All	All	All
Application	Invisioncommunity	Invision Power Board	3.3.2	All	All	All
Application	Invisioncommunity	Invision Power Board	3.3.3	All	All	All
Application	Invisioncommunity	Invision Power Board	3.3.4	All	All	All
Application	Invisioncommunity	Invision Power Board	3.4.0	All	All	All
Application	Invisioncommunity	Invision Power Board	3.4.0	alpha1	All	All
Application	Invisioncommunity	Invision Power Board	3.4.0	beta1	All	All
Application	Invisioncommunity	Invision Power Board	3.4.0	beta2	All	All
Application	Invisioncommunity	Invision Power Board	3.4.0	beta3	All	All
Application	Invisioncommunity	Invision Power Board	3.4.0	beta4	All	All

Application	Invisionpower	lp.nexus	1.5.4	All	All	All
Application	Invisionpower	lp.nexus	1.5.5	All	All	All
Application	Invisionpower	lp.nexus	1.5.6	All	All	All
Application	Invisionpower	lp.nexus	1.5.7	All	All	All
Application	Invisionpower	lp.nexus	1.5.8	All	All	All
Application	Invisionpower	lp.nexus	1.5.9	All	All	All
Application	Invisionpower	lp.nexus	1.5.0	All	All	All
Application	Invisionpower	lp.nexus	1.5.1	All	All	All
Application	Invisionpower	lp.nexus	1.5.2	All	All	All
Application	Invisionpower	lp.nexus	1.5.3	All	All	All
Application	Invisionpower	lp.nexus	1.5.4	All	All	All
Application	Invisionpower	lp.nexus	1.5.5	All	All	All
Application	Invisionpower	lp.nexus	1.5.6	All	All	All
Application	Invisionpower	lp.nexus	1.5.7	All	All	All
Application	Invisionpower	lp.nexus	1.5.8	All	All	All
Application	Invisionpower	lp.nexus	1.5.9	All	All	All

References

Reference	Source	Link	Tags
IP.Board And IP.Nexus Arbitrary File Include and Cross Site Scripting Vulnerabilities	BID	www.securityfocus.com	
IP.Board 3.3.x, 3.4.x Security Update - News and Information - Invision Power Services	CONFIRM	community.invisionpower.com	Patch
www.christian-schneider.net/advisories/CVE-2014-3149.txt	MISC	www.christian-schneider.net	
SecurityFocus	BUGTRAQ	www.securityfocus.com	
IP.Board 3.4.x / 3.3.x Cross Site Scripting ≈ Packet Storm	MISC	packetstormsecurity.com	
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web](#)

[site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report